

Application Serial No. 09/800,173  
Response dated: December 7, 2007  
Further Reply to final Office Action of April 10, 2007  
and the Amendment filed October 10, 2007

E-2538

### **AMENDMENTS TO THE CLAIMS**

Please amend the claims by replacing the previous listing of claims with the following listing of claims.

### **LISTING OF THE CLAIMS**

Claims 1-26 (Cancelled).

Claim 27. (New) An apparatus for transmitting data to a target comprising: a means for updating, present on a distribution media, and further comprising data, data information and a cryptographic hash of said data information; a means for transmission between said distribution media and said target, a means for obtaining data information from said distribution media; and, a means for processing said first cryptographic hash of said data information; whereby said means for obtaining data information from said distribution media obtains said first cryptographic hash from said means for updating present on said distribution media, which first cryptographic hash is comprised of a unique data identifier, and is transmitted through said means for transmission to said means for processing, and which upon receipt of said first cryptographic hash of said data information compares said first cryptographic hash to a second cryptographic hash installed on said target in order to determine if said data should be transmitted to said target, said data being less than the content of a file when only portions of a file, and not the entire file itself, require updating, and

Application Serial No. 09/800,173  
Response dated: December 7, 2007  
Further Reply to final Office Action of April 10, 2007  
and the Amendment filed October 10, 2007

E-2538

wherein at least one cryptographic hash is generated at said target and is stored at said target; said stored cryptographic hash corresponding with the data of said target.

Claim 28. (New) A computer-implemented method for transmitting data to a target comprising transmitting a first cryptographic hash of data information, which first cryptographic hash is comprised of a unique data identifier, from a first distribution media to said target; comparing said first cryptographic hash in order to determine if data information should be transmitted to said target; transmitting said data information from a second distribution media, if necessary, to said target; comparing said data information with said target in order to determine if said data should be transmitted to said target, wherein said data determined to be transmitted to said target is less than the content of a file when only portions of a file, and not the entire file itself, require updating;

including preparing said data information from attributes of said data, said data information comprising an update index file, wherein said first cryptographic hash of data information comprises a cryptographic hash of said update index file, and wherein comparing said first cryptographic hash in order to determine if data information should be transmitted to said target includes comparing said cryptographic hash of said update index file.

Claim 29. (New) A computer-implemented method as in claim 28, further comprising obtaining data information from said second distribution media.

Application Serial No. 09/800,173  
Response dated: December 7, 2007  
Further Reply to final Office Action of April 10, 2007  
and the Amendment filed October 10, 2007

E-2538

Claim 30. (New) A computer-implemented method as in claim 29, wherein obtaining data information from said second distribution media further comprises using an http address to obtain data information.

Claim 31. (New) A computer-implemented method for transmitting data as in claim 28, wherein the first and second distribution media are the same.

Claim 32. (New) A computer-implemented method for transmitting data as in claim 28, wherein either the first and second distribution media at least partially comprises a network.

Claim 33. (New) A computer-implemented method as in claim 28, wherein said data comprises one or more software product files.

Claim 34. (New) A computer-implemented method as in claim 28, further comprising preparing said cryptographic hash from said data information.

Claim 35. (New) A computer-implemented method as in claim 28 further comprising transmitting said data from a third distribution media to said target.

Claim 36. (New) A computer-implemented method as in claim 35 wherein the third

Application Serial No. 09/800,173  
Response dated: December 7, 2007  
Further Reply to final Office Action of April 10, 2007  
and the Amendment filed October 10, 2007

E-2538

distribution media at least partially comprises a network.

Claim 37. (New) A computer-implemented method as in claim 36 further comprising editing data on said target in order to update data on said target.

Claim 38. (New) A computer-implemented method for transmitting data to a target comprising the steps of: providing a software product; preparing data information about said software product; preparing a first cryptographic hash of data information about said software product; which first cryptographic hash is comprised of a unique data identifier, storing said software product on a first distribution media; storing said data information on a second distribution media; storing said first cryptographic hash of data information on a third distribution media; obtaining data information about said software product; transmitting said first cryptographic hash of data information to said target; comparing said first cryptographic hash to a second cryptographic hash installed on said target in order to determine if data information should be transmitted to said target; transmitting said data information, if necessary, to said target; comparing said data information with said target in order to determine if said data should be transmitted to said target; transmitting said data, if necessary, to said target; and, editing said data on said target in order to update data on said target.

Claim 39. (New) An apparatus for transmitting data to a target comprising: a means for updating, present on a distribution media, and further comprising data, data

Application Serial No. 09/800,173  
Response dated: December 7, 2007  
Further Reply to final Office Action of April 10, 2007  
and the Amendment filed October 10, 2007

E-2538

information and a first cryptographic hash of said data information; a means for transmission between said distribution media and said target, a means for obtaining data information from said distribution media; and, a means for processing said first cryptographic hash of said data information; whereby said means for obtaining data information from said distribution media obtains said first cryptographic hash from said means for updating present on said distribution media, which first cryptographic hash is comprised of a unique data identifier, and is transmitted through said means for transmission to said means for processing, and which upon receipt of said first cryptographic hash of said data information compares said first cryptographic hash to a second cryptographic hash installed on said target in order to determine if said data should be transmitted to said target, said data transmitted to said target comprising an editing command for editing said target.

Claim 40. (New) An apparatus for transmitting data to a target comprising: a means for updating, present on a distribution media, and further comprising data, data information and a first cryptographic hash of said data information; a means for transmission between said distribution media and said target, a means for obtaining data information from said distribution media; and, a means for processing said first cryptographic hash of said data information; whereby said means for obtaining data information from said distribution media obtains said first cryptographic hash from said means for updating present on said distribution media, which first cryptographic hash is

Application Serial No. 09/800,173  
Response dated: December 7, 2007  
Further Reply to final Office Action of April 10, 2007  
and the Amendment filed October 10, 2007

E-2538

comprised of a unique data identifier and is transmitted through said means for transmission to said means for processing, and which upon receipt of said first cryptographic hash of said data information compares said first cryptographic hash to a second cryptographic hash installed on said target in order to determine if said data should be transmitted to said target, wherein said data transmitted to said target comprises a binary editing command.

Claim 41. (New) A computer-implemented method for transmitting data to a target comprising the steps of: providing a software product; preparing data information about said software product; preparing a first cryptographic hash of data information about said software product; which first cryptographic hash is comprised of a unique data identifier, storing said software product on a first distribution media; storing said data information on a second distribution media; storing said first cryptographic hash of data information on a third distribution media; obtaining data information about said software product; transmitting said first cryptographic hash of data information to said target; comparing said first cryptographic hash to a second cryptographic hash installed on said target in order to determine if data information should be transmitted to said target; transmitting said data information, if necessary, to said target; comparing said data information with said target in order to determine if said data should be transmitted to said target; transmitting said data, if necessary, to said target; and, editing said data on said target in order to update data on said target, wherein said transmitted data comprises one or the

Application Serial No. 09/800,173  
Response dated: December 7, 2007  
Further Reply to final Office Action of April 10, 2007  
and the Amendment filed October 10, 2007

E-2538

other or both of (i) portions of a file and (ii) an editing command to effectuate a change in a file.

Claim 42. (New) The method of claim 27, wherein said data information comprises a module name and a hash of a module name, and wherein said first cryptographic hash is a hash of said data information.

Claim 43. (New) The method of claim 42, wherein said data comprises one or more modules, wherein upon transmission of said data to said target, an update manager performs the steps of extracting said one or more modules and replacing files or byte sequences, wherein said one or more modules contain directions for replacement of byte sequences.